16 September 2020

Input to the Consultation on the European Data Protection Board's Guidelines 6/2020 on the interplay of the PSD2 and the GDPR

We welcome the European Data Protection Board ('EDPB') 'Guidelines on the interplay of the Second Payment Services Directive ('PSD2') and the GDPR' (the 'Guidelines'), adopted on 17 July 2020, and the opportunity to respond to this consultation.

The PSD2's new legal framework for payment services and data sharing standards has encouraged the creation of innovative new services which have led to broader access to payment services. The legislation is enabling financial inclusion and stimulating competition, whilst increasing the protection of individuals against fraud and the misuse of their personal data.

Although effective on 14 September 2019, implementation of the PSD2 remains in early stages. Meanwhile, the market is evolving, and consumer expectations change rapidly, particularly in the face of all the transformations brought on by the pandemic over the course of 2020. Despite a number of uncertainties, what is clear is that the development of new services and business models as part of the new Open Banking ecosystem depends on access to personal data and data sharing.

We appreciate that the Guidelines aim to clarify this new complex legal environment. There is a need to set fair, ethical, accountable, and legally compliant conditions to enable the further development of this ecosystem while enabling individuals to benefit from new solutions that provide high data protection standards.

Innovation is critical to business success, but not at the expense of the ethical use of data. We therefore fully endorse the EDPB's emphasis on accountability and the need to embed privacy safeguards (including transparency and data minimisation), into the design of all payment and Open Banking services, products and technologies.

Considering this, our response to the EDPB Guidelines on the interplay of the PSD2 and the GDPR, focuses on:

I. **Further processing should be permitted beyond strict consent or legal necessity legal basis.** Further processing of personal data for compatible purposes in the context of payment initiation and account information services of silent party data should be permitted not only based on consent or EU or Member State law. PSD2 should not be interpreted to selectively limit the applicability of the GDPR. The conditions for further processing require consideration of factors such as the link with the initial purpose, context, impact on individuals, and implementation of appropriate safeguards. It is up to each data controller to consider these factors and the risks involved with further processing.

II. **Payment and account information data should not inherently be treated as special category of data.** The purpose and the context of the processing should be the determining factor in assessing whether special categories of data are being processed as part of payment initiation and account information services. We would welcome clearer alignment with current EDPB and supervisory authority interpretations which indicate that while payment and account information may possibly reveal special category data through inferences, it would be inappropriate to treat payment and account information *inherently* as special category data.

III. **Overlapping transparency requirements in the context of explicit consent should be avoided.** While we welcome the consistency in clarifying that consent in the PSD2 is a contractual consent and different from consent under the GDPR, we would like to avoid overlapping transparency requirements between the GDPR and PSD2. Privacy notices should be holistically used to properly inform individuals about data processing and their privacy rights. Any additional data protection information should not be included in the contract with the Payment Service User ('PSU').

IV. **Clearer data minimisation guidance is needed.** While we welcome the EDPB's emphasis on accountability and privacy enhancing technologies, we would appreciate clear affirmation that it is

up to each data controller to determine the scope of data minimisation in relation to the intended purposes and the risks involved. Any suggestion that data should be redacted before it is provided to a Payment Initiation Service Provider ('PISP) or Account Information Service Provider ('AISP'), and special category data removed, should be avoided. Such a recommendation would conflict with the obligations under PSD2 and the Regulatory Technical Standards for Strong Customer Authentication ('SCA RTS'), which requires that the same information is provided to an AISP as it would be made available to a PSU.

I. Further processing should be permitted beyond strict consent or legal necessity legal basis

The Guidelines establish that PSD2 restricts the possibility for further processing, unless the data subject has given consent, or the processing is provided for by Union law or Member State law to which the controller is subject. Any subsequent further processing would be considered automatically incompatible with the initial purpose. This would be the case even if there is a link with the initial purpose, consumers have reasonable expectations that such processing takes place, and necessary safeguards have been put in place.

There are legal and practical implications of this interpretation:

1. **Hierarchy of legal norms.** Both the GDPR and PSD2 create separate legal regimes. One is neither supreme to the other, nor *lex specialis*. Likewise, the difference in form of secondary legislation (Regulation vs Directive) creates no superiority between them.

   This means that PSD2 should not be interpreted in a way that selectively limits the applicability of certain GPPR provisions, as there is no explicit mandate to do so in the PSD2. Instead, both legal acts should be interpreted and applied in a manner that enables compliance with both laws and preserves their specific and unique purpose. This approach is confirmed by the Court of Justice (*CJEU in C-73/17 France v European Parliament*), which held that where two legal norms have the same legal value, the obligations of one norm cannot prevail over the other. The application of the norms *"must be on a case-by-case basis and in a manner that reconciles those obligations and strikes a fair balance between them*".

   The requirements of Article 6(4) GDPR help assess what types of further processing should be allowed, specifically low risk processing and processing for the purpose of the prevention and protection of fraud. Any other interpretation would create a dangerous precedent of not applying one of the fundamental principles of the GDPR, i.e., the equal footing of the permitted legal bases for data processing. This would disturb the level playing field intended by GDPR and would put the financial industry at a disadvantage compared to other businesses.

2. **Functional relationship between the PSD2 and the GDPR.** PSD2 and GDPR constitute at their cores two distinct and yet overlapping regimes, both impacting the use of data (personal data and/or payment data), which apply different concepts, whilst sometimes using the same words with different objectives. While PSD2 is centred around the concept of 'services', the GDPR relies heavily on the concept of 'purposes'. For that reason, Annex I of the PSD2 sets out an exhaustive list of types of payment services. The reminder in Articles 66(2)(g) and 67(2)(f) to 'not use, access or store any data for **purposes** other than for performing the [account information service/ payment initiation service][…]' therefore clearly allows the use of data for multiple purposes as long as they relate to the payment service. This is logical as **a single service under PSD2 may comprise of multiple processing purposes under the GDPR**.

   The GDPR allows a data controller to process personal data for multiple purposes in the context of a relationship and these purposes may rely on various legal grounds, such as legitimate interest, if they meet relevant requirements. This is consistent with the Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, which provides that where some services cannot be justified by contractual necessity, they may still be justified by legitimate interests if relevant requirements have been met (e.g. paragraph 37 of the 2/2019 Guidelines). This would be also

consistent with the current Guidelines which recognise in paragraph 8 that several different types of services can be offered with different features and purposes.

In this context, the application of Article 6(4) GDPR remains appropriate as dependent on the actual legal grounds for the specific purpose of the processing related to the payment service, further compatible purposes should be allowed in line with recital 50 of the GDPR.

3. **Types of Open Banking services in the PSD2.** The PDS2 recognises and reflects in its provisions the difference between payment initiation services and account information services. The nature of payment initiation services is simple, i.e., to initiate a payment. The purpose of account information services is to make payment and account data available for information services and allow for account aggregation benefitting the PSU. Notably, the explicit reference in Article 67(2)(f) to data protection rules should be considered with this perspective in mind. On its natural reading, it would allow further processing in accordance with Article 6(4) of the GDPR and would not restrict data protection rules. Importantly, Article 67(2)(f) refers to data protection rules (in general) and not to selective GDPR provisions.

4. **Processing for fraud prevention and monitoring purposes.** By allowing further processing only when it is based on consent or legal obligation, the Guidelines disregard the specific reference in Article 94(1) of the PSD2. This article provides a direct mandate to permit processing of personal data when this is necessary to safeguard the prevention, investigation and detection of payment fraud. Unfortunately, this Article may not be sufficiently specific to be qualified as a legal obligation under Article 6(1)(c) of the GDPR. The Guidelines should therefore either specifically indicate that Article 94(1) of the PSD2 provides such legal basis or allow further processing in line with Article 6(4) of the GDPR for the purposes of fraud prevention and monitoring. Note in this respect that the GDPR Recital 71 refers to fraud monitoring and prevention purposes conducted in accordance with regulations, standards and recommendations of union institutions or national oversights bodies.

5. **Further processing of silent party data.** A narrow approach that no further processing is permitted regarding silent parties' data would fail to acknowledge the complexities of the architecture of the Open Banking ecosystem, the nature and the dynamic evolution of financial services, the relationships between various stakeholders involved in the provision of these services, and the high level of data protection safeguards implemented by the financial industry. Further processing of silent party data remains essential to the developing Open Banking ecosystem. Realistically, each data controller would need to undertake case by case assessment, to ensure full compliance with GDPR and PSD2. Note that in this respect, Article 11 of the GDPR provides that controllers are not obliged to maintain, acquire or process additional information in order to identify the data subject.

Many data processing operations would not be possible without further changes to the guidance regarding further processing and the consequences could be far reaching for individuals and businesses. For example:

a) **Fraud detection and prevention.** Consumers have a reasonable expectation that the services they are seeking are secure and that entities involved in the payment initiation and account information services take the necessary measures to monitor, prevent and eradicate fraud. Fraud prevention solutions depend on the analysis of historical payment transaction information and data which is used to train these solutions to score potentially fraudulent activity.

Requiring consent in the context of fraud detection is not feasible, practical, or reliable. The security and stability of the payment systems cannot be made dependent on individuals' consent. Such consent would also not be workable in practice because many stakeholders that play an essential role in the protection of security and stability of payment systems do not have a direct relationship with the payment service users and may not be directly targeted by specific Union and/or Member state laws.

b) Data aggregation and anonymization. Data anonymization is often a separate processing activity which requires a lawful basis under the GDPR. If compatible processing would not be permitted under the Guidelines, the unintended consequence is that personal data processed

in the context of payment initiation and account information services cannot be anonymized to allow insights to be derived from it, even if it actually does not cause any risks to individuals. This is very unfortunate as responsible innovation through the use of aggregated and anonymized payment and account information for analytics and business development will drive economic development and enable the creation of reliable economic indicators benefiting economic recovery, including for populations hard hit by the COVID-19 pandemic.

c) **Personal finance management.** Further compatible processing of silent party data would allow individuals to properly manage their finances across financial institutions and build a legitimate financial profile, ultimately allowing for greater access to credit and better services. These potential features enabled through account information services present unique opportunities to increase financial inclusion of historically under-served consumers.

   For example, payment history, involving the processing of silent party data, may be used to augment traditional credit reference scoring. A consumer applying for a mortgage or other credit facility would be able to show consistent payment history in another area, such as rent repayments, maintenance payments, or regular payments to a dependent. This would require the lender to identify that the payment recipient (often an individual) is the same person for each monthly payment. Merely showing the same amount being transferred is not likely to be sufficient, as the same recipient would need to be identified (and amounts may slightly differ). This would require the processing of the silent party's personal data to track payments to them from the consumer's account. If further processing of the silent party was not permitted, such opportunities would be jeopardised.

We would welcome further clarification consistent with earlier EDPB guidelines that if the parties in the Open Banking ecosystem rely on the legal basis of performance of the contract for providing the account information of payment initiation services, it does not prevent them from relying on other legal bases for purposes related to the payment service, as long as the applicable criteria have been met.

Clarification is needed in the Guidelines that further processing is allowed when consistent with the requirements of Article 6(4) of the GDPR, in particular with respect to Article 67(2)(f). In that respect, data controllers must assess the risks involved with any further processing while understanding the new data use's link with the initial purpose for collection, as well as context, impact on individuals, and put in place appropriate organisational and technical safeguards.

We recommend that EDPB clarifies the relationship between Article 94(1) of the PSD2 and the nature of Recital 71 in the context of permitting further processing for fraud prevention and monitoring purposes, in relation to payment services.

II. Payment and account information data should not, by default, be treated as special category data

The Guidelines provide that payment transactions can reveal sensitive information, and in those situations must be classified as special category data. We believe that this interpretation is overly broad and far reaching and would have significant unintended consequences in practice. Moreover, we believe it is neither in line with the intent of the PSD2 nor supported by the earlier opinions of the EDPB, national supervisory authorities or current case law which take a teleological approach.

1. **Narrow scope of Article 9 of the GDPR**. Article 9 of the GDPR is an exception to the general principle that there is no hierarchy of personal data and that all personal data should be treated the same. Therefore, as an exception, Article 9 should be interpreted narrowly. The *ratio legis* of this provision is not to treat all personal data as potentially sensitive.

   Following on the EDPB's logic, potentially any information that can reveal sensitive information must be regarded as special category data even where it does not explicitly do so. For example:

   - First names and family names often reveal ethnic origin or religion;

- Address can reveal ethnic origin and sometimes sexual orientation (i.e. certain areas are predominantly populated by certain ethnic groups, certain community living buildings are specifically dedicated to individuals with certain sexual orientation);
- Location data will reveal health, religion, or sexual orientation, when it concerns the location of religious buildings, hospitals, workers' union's premises;
- Pictures reveal race and ethnic origin and may indicate health/ physical impairments (e.g. photos with head coverings, persons in a wheelchair).

None of these and other similar types of data are systemically regarded as special category data, either by the EDPB, or by the national courts, or by national supervisory authorities. We specifically refer to the Dutch constitutional court's decision regarding video images (ECLI:NL:HR:2017:1166 - Hoge Raad, 27-06-2017 / 15/05012) of 26 June 2017 which confirms that video footage is not by default special category data except if additional processing is undertaken to derive sensitive information. This **teleological interpretation**, dependent on the purpose of the actual processing taking place, is confirmed by Recital 51 of the GDPR in respect of photos.

2. **Consistency with EDPB and national supervisory authority interpretation of special category data.** The EDPB appears to confirm that the context and the purpose of the processing determines whether the processing of special category data takes place where the data itself is not explicitly special category data. In the recent Guidelines 08/2020 on the targeting of social media users, the EDBP has clarified the nature of special categories of personal data indicating that it is the additional processing activity by the data controller, which determines that the processing of special category data takes place.

   The EDPB stated that such processing of special category data could take place if such personal data are combined with other data or because of the context in which the personal data are processed or the purposes for which they are being used. Furthermore, the EDPB provided that even large-scale processing of data which potentially could be used to infer special category data does not automatically mean that the processing falls under Article 9 of the GDPR. Article 9 will not be triggered if the processing does not result in inference of special category data and the social media provider has taken measures to prevent that such data can be inferred or used for targeting (paragraph 117).

   The Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), referred to the inference of special category data from other data which is not special category data in its own right, but becomes so when combined with other data.

   The UK Information Commissioner's Office has clarified that whether any inference could count as special category data depends on how certain that inference is, and whether the data controller is deliberately drawing that inference (ICO Guidelines on special category data). A possible inference or an 'educated guess', is not a special category data, unless the personal information is specifically processed to treat someone differently on the basis of that inference, for example through profiling techniques.

   Dutch supervisory authority's guidelines on camera surveillance provide another example of current guidelines (see here and here). These guidelines specifically allow for processing of camera footage based on legitimate interest as long as specific safeguards are in place, such as transparency, data minimisation and a DPIA has been undertaken.

   Similarly, payment and account information do not explicitly reveal special category data. Rather it is up to each data controller to assess whether it is, or it potentially might be, processing such data by looking into the specific type of data processing activity. This includes an analysis for the purpose of profiling, as the EDPB itself indicates for health data in paragraph 51 of the Guidelines: *"Personal data concerning health may be gathered from analysing medical bills paid by a data subject".*

Qualifying certain payment and account information as special category data will have a significant impact on the payment ecosystem which poses **a number of serious practical challenges:**

a) Due to the nature of the flow of payment and account information, multiple stakeholders in the payment ecosystem would find it impossible to assess the purpose of a payment or have information about such purpose. For example, a payment to a hospital can in certain instances indicate payment of medical treatment but could also be a payment by a hospital restaurant service for allowing the use of its premises. Donation to a research project organised by a catholic university will not automatically reveal that a donor is Catholic. Similarly, donation to a cancer charity does not mean that a donor has cancer.

b) No technical measures are currently available to assess the purpose of each payment and even less on a real-time basis. Thus, every payment capable of revealing special category data would have to be treated as processing special category data under the GDPR and would, as the EDPB notes in the Guidelines, require explicit consent unless the processing can be based on substantial public interest. Unfortunately, it would be impossible to obtain explicit consent in practice as it needs to be specific and informed and would require many separate explicit consents to be obtained. It would also go against the expectations of the users, who want instant and secure services and payments without additional hurdles or clicks along the way. In addition:

    i. Two consents would always be required: a GDPR explicit consent and the contractual Article 94(2) consent under PSD2. Parties would have to collect different consents multiple times for separate purposes, disturbing the user experience and generating confusion about the use of their personal data.

    ii. It would be unclear what the consequences would be of withdrawal of the GDPR explicit consent. Would payment initiation and account information services need to be terminated even if the contractual engagement continues and payment transactions need to be refused or revoked?

c) Some examples in the Guidelines seem to indicate that the recipient of any payment, and not the purpose of the processing of the payment or account information determines whether it is special category data. In that respect, is not clear how data minimisation could be achieved. Would the Guidelines actually require that recipients such as churches, religious schools, religious publishing houses, hospitals, pharmacies, etc., be masked and information about such recipients not be further processed?

The approach to qualifying payment and account information as a special category data should be better aligned with current case law, and existing EDPB and national supervisory authority guidelines and more pragmatic and nuanced. We would specifically welcome alignment with current interpretations in the context of social media or profiling, without singling out payment and account information.

The purpose of the processing should determine whether special category data are being processed in relation to payment initiation and account information services, given that the data is not explicitly special category data. Whether personal data is special category or not should depend on the context and finality of the processing. In other words, when processing account and payment data relating to medical services, payment data should not be considered as special category data if the purpose is to provide typical AISP and the/or PISP services. Such processing could, however, qualify as special category data if the purpose is to analyse all medical information for further profiling/analytics activities.

III. Overlapping transparency requirements in the context of explicit consent should be avoided

We welcome the confirmation of the earlier EDPB opinion that explicit consent in Article 94(2) of the PSD2 is a contractual consent and different from explicit consent under the GDPR. We appreciate this clarification as a different interpretation of the PSD2 would have caused significant practical disruptions in the functioning of payment initiation and account information services. We also appreciate that the EDPB has taken this position at the outset, even before the implementation deadline of PSD2, which

has greatly facilitated our privacy by design approach related to the development of payment initiation and account information services.

However, the additional requirements laid out in the Guidelines for the validity of such contractual consent, i.e., additional transparency, raise some practical considerations:

1. **The relationship between the regular privacy notice under GDPR and the additional 'privacy information'** to be provided as required by the guidelines creates confusion for businesses and individuals. It is not clear whether the 'privacy information' under Article 94(2) contains the same information as typically would be provided in the privacy notice under GDPR, for example as a subset of the GDPR privacy notice.

2. **Expectations regarding further privacy information.** If the additional 'privacy information' would contain more or different explanations, it is unclear what the expectations are in respect of and what granularity of the information must have. Would the EDPB guidelines on transparency also be applicable to this 'privacy information'? Individuals need practical and transparent information in easy-to-recognise formats which they can refer to. Disparate information provided in different manners would confuse individuals and negatively impact their understanding of payment initiation and account information services.

We believe for practical and consistency reasons that controllers should typically use the format of privacy notices to properly inform individuals about the data processing and their privacy rights. Any additional privacy information required by the EDPB should not be included in the contract with the PSU. We believe that any additional requirement to the contrary would cause information fatigue and run directly counter to the EDPB's goals of enhanced transparency.

IV. Clearer data minimisation guidance is needed

We welcome the EDPB's emphasis on organisational and technical privacy enhancing measures, including transparency and data minimisation. These are necessary safeguards to protect individuals that allow for further innovation benefitting individuals. We fully adhere to the use of technology to help data controllers meet their obligations and enhance their accountability in respect of privacy and data protection.

Under the GDPR it is up to each data controller to undertake its own assessment and determine the scope of data minimisation in relation to the intended purposes and the risks involved, in compliance with any applicable rules and regulations. However, the Guidelines appear to suggest that the Account Servicing Payment Service Providers ('ASPSP') should redact certain data, including special category data from payment and account information, and thus limit data sharing with PISPs and AISPs thereby effectively monitoring the personal data sets to be provided to AISP.

Requiring ASPSPs to minimise and redact the payment and account information before sharing with PISPs and AISPs, as required under the Guidelines, would have severe legal and practical consequences:

1. **ASPSPs would be in direct violation of the PSD2.** Under the PSD2, the AISP needs to be allowed access without discrimination to the same data that the PSU would normally access. The SCA RTS requires that ASPSPs provide "*the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data*" (Article 36 Data exchanges). The PSD2 and the SCA RTS exclude access to sensitive payment data but do refer to other categories of data. Therefore, such minimisation to exclude special category data by default is not justified.

2. **Transparency and data usability**. Limiting the information available to the AISP would impact the usability of the data and transparency for the PSU and thereby undermine the purpose of PSD2. It would also impair the reliability of the services provided by AISPs as these services would be based on partial data sets. It would create incessant conflicts and procedures about AISPs' unnecessary and unwanted data redaction.

We would welcome a clear acknowledgment that each data controller is responsible for implementing appropriate organisational and technical measures, including data minimisation in respect of its own personal data processing activities, contrary to any data sharing obligations it may have with respect to third parties.

Concluding remarks

We greatly appreciate the EDPB's analysis of the complex relationships between data protection and the payment services legal framework. The EDPB is setting the path for how the payment services sector and its connected industries will evolve in the coming years in compliance with privacy and data protection rules. More clarity regarding the fundamental aspects of the GDPR in the context of the PSD2 will help ensure consistency in the interpretation of the GDPR. Moreover, this will lead to increased accountability while safeguarding the intention and purpose of both legal regimes. We are looking forward to further engaging with the EDPB on this topic and to provide further insights on the practical implications of the EDPB's considerations.

Developments in the payment ecosystem are dynamic and ever evolving. They correspond with customers' new expectations for Open Banking and the ability of the industry to match these expectations. As the EU drives towards stimulating data sharing, we are mindful that an unnecessarily restrictive approach to PSD2 could have a stifling effect on innovation. Overregulating the market or imposing unnecessary onerous requirements runs the risk of undermining the full potential of PSD2 and its benefits to individuals. As highlighted in the opening remarks, PSD2 became effective only a year ago and this is still a new market.

We believe that the full potential of PSD2 can be attained while providing adequate privacy protection to individuals in line with the GDPR and we believe that the EDPB's Guidelines will be essential in this respect.